

Signing Information

Page 1/1

 Redegjorelse_apenhetsloven_2026 .docx.pdf

Name:	Method:	Time:
Friis, Kjartan Nielsen	BANKID	2026-05-12 09:38:55
Sommerseth, Martin Hagen	BANKID	2026-05-12 20:02:19
Karlsson, Christina	BANKID	2026-05-12 08:58:51
Grønlund, Julie Katrine Groth	BANKID	2026-05-11 16:26:22



This document is electronically sealed and contains electronic signatures

Document ID:9e1945d2-5244-4f16-945a-894d9032aa74

2026: Redegjørelse for aktsomhetsvurderinger etter åpenhetsloven

House of Control AS

Rapporteringsperiode: juli 2025 – juni 2026

Innledning

Denne redegjørelsen er utarbeidet i henhold til lov om virksomheters åpenhet og arbeid med grunnleggende menneskerettigheter og anstendige arbeidsforhold (åpenhetsloven).

Formålet med redegjørelsen er å gi allmennheten innsikt i hvordan House of Control jobber systematisk med aktsomhetsvurderinger for å identifisere, forebygge og redegjøre for vår faktiske og potensielle påvirkning på grunnleggende menneskerettigheter og anstendige arbeidsforhold – både i egen virksomhet og i vår leverandørkjede.

For House of Control er dette arbeidet ikke bare et lovkrav, men en integrert del av hvordan vi ønsker å drive virksomhet. Som leverandør av programvare for blant annet etterlevelse av åpenhetsloven, anser vi det som strategisk viktig å gå foran med et systematisk og dokumentert eget arbeid på området.

Redegjørelsen dekker perioden juli 2025 – juni 2026 og er, sammen med våre styrende dokumenter, tilgjengelig for allmennheten på vår nettside: [Slik jobber vi med åpenhetsloven](#).

Om House of Control

House of Control er et programvareselskap (SaaS) som utvikler og selger løsninger for blant annet avtalehåndtering, IFRS 16-rapportering, DORA-etterlevelse og overholdelse av åpenhetsloven. Våre kunder er primært private og offentlige virksomheter i Norden. House of Control er en del av Visma-konsernet.

Denne redegjørelsen omfatter aktsomhetsvurderinger for hele vår nordiske virksomhet. Antall ansatte per juni 2026 er fordelt som følger:

- House of Control AS (Norge): 59 ansatte
- House of Control Sverige AB (Sverige): 9 ansatte
- House of Control Danmark A/S (Danmark): 7 ansatte

Tallene gjelder fast ansatte og ekskluderer eksterne konsulenter. I tillegg til våre ansatte benytter virksomheten jevnlig innleide konsulenter, primært innen systemutvikling. For rapporteringsperioden utgjør dette i gjennomsnitt 9 konsulenter. Vårt ansvar for å bidra til anstendige arbeidsforhold for disse ivaretas gjennom kravene vi stiller til konsultantselskapene i vår Supplier Code of Conduct, samt gjennom løpende oppfølging av kontraktene.

Forankring, retningslinjer og rutiner

Arbeidet med åpenhetsloven er forankret i selskapets ledelse og styre, og ansvaret for utarbeidelse og godkjenning av den årlige redegjørelsen ligger hos daglig leder. Vår tilnærming bygger på OECDs retningslinjer for flernasjonale selskaper og er integrert i våre interne styringssystemer. Arbeidet bygger på det etablerte rammeverket i Visma-konsernet, som er nærmere beskrevet i

[Vismas bærekraftsrapport](#).

Vårt eget rammeverk består av flere sentrale dokumenter:

- **Human Rights Statement:** Dokumentet fastslår vår forpliktelse til å respektere internasjonalt anerkjente menneskerettigheter i tråd med FNs og ILOs konvensjoner.
- **Supplier Code of Conduct:** Våre etiske retningslinjer for leverandører setter klare minimumskrav til våre forretningspartnere, basert på konsernets felles [Supplier Code of Conduct](#)
- **Anti-Corruption Policy:** Vi har nulltoleranse for korrupsjon, i tråd med konsernets felles etiske retningslinjer. I rapporteringsperioden har vi også gjennomført en oppdatert korrupsjonsrisikoanalyse som dekker hele virksomheten, med definerte tiltak og risikoansvarlige.
- **Plan for aktsomhetsvurderinger:** Vi har en intern plan som beskriver hvordan aktsomhetsvurderinger gjennomføres, prioriteres og følges opp. Planen er oppdatert i 2026 og gjennomgås årlig.

Aktsomhetsvurderinger i praksis

Kjernen i redegjørelsen er dokumentasjonen av selve aktsomhetsarbeidet. Vi har i denne rapporteringsperioden videreutviklet våre rutiner for å sikre en mer systematisk og sporbar prosess.

Oppdaterte interne rutiner

I løpet av rapporteringsperioden har vi revidert vår interne veiledning for aktsomhetsvurdering av leverandører. Endringene innebærer blant annet:

- Tydeligere ansvarsfordeling der avtaleansvarlige har et definert ansvar for å gjennomføre risikovurdering ved inngåelse av nye avtaler og ved vesentlige endringer.
- En strukturert årlig revisjonssyklus for våre mest vesentlige leverandører, hvor risiko vurderes på nytt basert på blant annet bransje, geografi, leveransens karakter og tidligere observasjoner.
- Bruk av selskapets egen plattform Complete Control for innsamling, dokumentasjon og oppfølging av leverandørundersøkelser, noe som sikrer sporbarhet og en konsolidert oversikt over leverandørporteføljen.
- Klarere kriterier for prioritering av oppfølging basert på risikoens alvorlighetsgrad og sannsynlighet, samt selskapets påvirkningsmulighet.

Den oppdaterte rutinen sikrer at aktsomhetsvurderinger ikke er en engangshendelse, men en kontinuerlig prosess som inngår i den løpende leverandøroppfølgingen.

Risiko og funn

I vårt arbeid med aktsomhetsvurderinger har vi kartlagt våre leverandørkjeder for å identifisere, forebygge og begrense negativ påvirkning. Som et programvareselskap ligger

vår mest vesentlige potensielle risiko i de globale leverandørkjedene for teknologi – spesielt knyttet til produksjon av maskinvare og levering av skytjenester.

Under følger anonymiserte eksempler på hvordan vi har vurdert risiko og iverksatt tiltak overfor sentrale leverandørtyper i rapporteringsperioden. I tråd med åpenhetsloven § 5 oppgis ikke navn på enkeltleverandører, blant annet av hensyn til forretningsmessige forhold og forhold som angår leverandøren selv.

Eksempel 1: Vurdering av global skyleverandør og drift av datasenter

House of Control benytter en verdensledende, global aktør som strategisk leverandør for skytjenester. Tilnærmet alle våre kunder leveres på denne plattformen. Det er viktig å presisere at vi kjøper en digital tjeneste – ikke fysisk utstyr.

Identifisert potensiell risiko: Leveransen av skytjenesten er avhengig av en omfattende fysisk infrastruktur som skyleverandøren selv anskaffer, bygger og drifter. Den potensielle risikoen vi har vurdert er derfor indirekte og knyttet til to forhold i vår leverandørs verdikjede:

- **Produksjon av maskinvare:** Anskaffelse av servere, lagringsenheter, nettverkskomponenter og annet IT-utstyr skjer gjennom en global og kompleks leverandørkjede. Produksjon av elektronikk er internasjonalt anerkjent som en høyrisikobransje, blant annet knyttet til arbeidstid, lønnsvilkår, helse og sikkerhet i produksjonen, samt utvinning av råvarer som mineraler og metaller (såkalte konfliktmineraler).
- **Drift av datasentre:** Arbeidsforholdene for personell som bygger, vedlikeholder og drifter de fysiske datasentrene utgjør en potensiell risiko. Dette omfatter både egne ansatte hos skyleverandøren og innleid personell fra entreprenører og underleverandører som utfører bygge-, sikkerhets-, renholds- og driftsoppgaver på datasentrene.

Gjennomførte tiltak (aktsomhetsvurdering): Da vår påvirkningsmulighet er indirekte, er vårt hovedtiltak å forsikre oss om at skyleverandøren har robuste, egne systemer for å håndtere disse risikoene. Vi har i rapporteringsperioden gjennomgått leverandørens offentlig tilgjengelige forpliktelser, herunder:

- Offentlig publiserte retningslinjer for ansvarlig leverandørkjede (Supply Chain Standards / Supplier Code of Conduct), inkludert krav til arbeidsforhold, forbud mot tvangs- og barnearbeid, og forventninger om sporbarhet av mineraler.
- Leverandørens årlige bærekrafts- og menneskerettighetsrapportering, hvor de redegjør for sin egen tilnærming til aktsomhetsvurderinger og resultatet av disse.
- Sertifiseringer og tredjepartsrevisjoner av datasenterdriften, herunder ISO-standarder for informasjonssikkerhet og driftsmiljø.

Vi har dessuten strategisk valgt å benytte leverandørens datasenterregion i Norden for alle våre nordiske kunder. Dette tiltaket reduserer den geografiske risikoen vesentlig, da driften er underlagt nordisk og europeisk arbeidslovgivning, herunder bestemmelser om lønns- og arbeidsvilkår, organisasjonsfrihet, arbeidsmiljø og diskrimineringsvern. For kunder i

Storbritannia benyttes regionen i London, som er underlagt tilsvarende britisk arbeidsmiljølovgivning.

I tillegg har vi i rapporteringsperioden gjennomgått selskapets oversikt over underleverandører (sub-processors) i forbindelse med GDPR-arbeidet. Denne kartleggingen gir også et nyttig bidrag til aktsomhetsarbeidet, ettersom den synliggjør hvor vesentlige data lagres og hvilke aktører som er involvert i leveransen av tjenestene våre.

Konklusjon: Vår vurdering er at skyleverandøren har tilfredsstillende systemer for å identifisere og håndtere de indirekte risikoene knyttet til både produksjon av maskinvare og drift av datasentre. Vi følger leverandørens offentlige rapportering for å fange opp eventuelle endringer i risikobildet, og vil ved vesentlige funn vurdere ytterligere tiltak eller dialog med leverandøren.

Eksempel 2: Vurdering av forhandler av maskinvare

Vi benytter en stor, nordisk forhandler for innkjøp av IT-utstyr som PC-er, skjermer og tilbehør til våre kontorer i Norden.

Identifisert potensiell risiko: Risikoen ved dette innkjøpet ligger ikke hos den nordiske forhandleren, men hos produsentene av utstyret de selger. Produksjon av elektronikk er en global høyrisikobransje. I tillegg utgjør elektronisk avfall (e-avfall) en betydelig risiko for menneskerettigheter dersom det ikke håndteres på en forsvarlig måte ved slutten av levetiden, særlig knyttet til uformell resirkuleringsindustri i enkelte deler av verden.

Gjennomførte tiltak (aktsomhetsvurdering): Vårt hovedtiltak er å forsikre oss om at forhandleren gjennomfører egne grundige aktsomhetsvurderinger av sine produsenter. Vi har gjennomgått forhandlerens bærekraftsrapport, som bekrefter at de stiller krav til sine leverandører i tråd med internasjonalt anerkjente standarder. Kravene i vår egen Supplier Code of Conduct er formidlet til forhandleren, og forhandleren har bekreftet at de driver i samsvar med disse.

Vi benytter aktivt forhandlerens tjenester for tilbakekjøp og ansvarlig håndtering av brukt IT-utstyr. Dette sikrer at utstyret blir dataslettet på en trygg måte, og at det enten gjenbrukes eller resirkuleres gjennom forsvarlige kanaler. Tiltaket reduserer risikoen for at vårt e-avfall bidrar til uverdige arbeidsforhold.

Konklusjon: Vi anser at forhandleren har gode rutiner for å håndtere risiko knyttet til både maskinvareproduksjon og produktenes livsløp, og at det er forsvarlig å fortsette innkjøp gjennom dem.

Eksempel 3: Endringer i tjenester for renhold og kantine

Renhold er en bransje som internasjonalt og nasjonalt er forbundet med risiko for sosial dumping, uverdige lønns- og arbeidsvilkår, samt mangelfull oppfølging av arbeidsmiljølovgivning. Tilsvarende kan kantinetjenester og bemanning gjennom innleieselskaper innebære risiko knyttet til midlertidighet og lønnsvilkår.

Identifisert potensiell risiko og funn: Gjennom våre aktsomhetsvurderinger har vi vurdert risikoen for at vi gjennom våre innkjøp av renhold- og kantinetjenester indirekte kunne bidra til uverdige arbeidsforhold. Dette gjelder særlig kombinasjonen av lavtlønnsyrker, høy andel utenlandsk arbeidskraft og flernivå-underleverandørstrukturer i deler av bransjen.

Gjennomførte tiltak: På bakgrunn av vurderingen har House of Control i rapporteringsperioden valgt å ansette personell direkte i House of Control fremfor å benytte innleid personell eller eksterne tjenesteleverandører for disse oppgavene. Denne strukturelle endringen gir oss full kontroll over arbeidsforhold, lønnsvilkår, opplæring og arbeidsmiljø, og fjerner risikoen for indirekte bidrag til uverdige arbeidsforhold gjennom underleverandører.

Konklusjon: Etter omleggingen anser vi at vi har redusert risikoen vesentlig på dette området. Forhold knyttet til renhold og kantine vurderes nå som en del av vår egen virksomhet, og er omfattet av selskapets ordinære HR-prosesser, arbeidsmiljøarbeid og internkontroll.

Vurdering av egen virksomhet

House of Control er forpliktet til å sikre et trygt, rettferdig og inkluderende arbeidsmiljø for alle våre ansatte i Norge, Sverige og Danmark. Vi vurderer at risikoen for brudd på grunnleggende menneskerettigheter og anstendige arbeidsforhold i egen virksomhet generelt er lav, men har en helhetlig tilnærming for å sikre at risikoen håndteres aktivt.

Arbeidsmiljø og medvirkning

Vi gjennomfører jevnlig medarbeiderundersøkelser for å fange opp forhold knyttet til arbeidsmiljø, psykososialt arbeidsmiljø, arbeidsbelastning og trivsel. Resultatene følges opp av ledelsen og benyttes som grunnlag for forbedringstiltak. Vi har etablerte samarbeidsstrukturer med ansattes representanter, og legger til rette for at ansatte kan ta opp forhold som angår eget arbeidsmiljø, både formelt og uformelt.

Likestilling, mangfold og ikke-diskriminering

Vi arbeider aktivt og målrettet for likestilling og mot diskriminering, i tråd med kravene i likestillings- og diskrimineringsloven. Selskapet har interne rutiner for å sikre rettferdig lønnsfastsettelse, like utviklingsmuligheter og at rekruttering, forfremmelse og kompetanseutvikling skjer på et likeverdig grunnlag uavhengig av kjønn, alder, etnisitet, religion, legning, funksjonsevne eller andre personlige forhold. Disse prosessene følges opp årlig.

Helse, sikkerhet og arbeidstid

Som teknologiselskap er våre vesentligste arbeidsmiljørisikoer knyttet til psykososiale forhold, langvarig skjermarbeid og arbeidsbelastning. Vi har rutiner for ergonomi, fleksibel arbeidstid, og vi følger lovkrav til arbeidstid i alle tre land. Arbeidsmiljøutvalg og verneombud bidrar til å forebygge og håndtere helse- og sikkerhetsrelaterte forhold.

Etikk, opplæring og antikorrupsjon

Alle ansatte er omfattet av selskapets etiske retningslinjer. I rapporteringsperioden har vi gjennomgått og oppdatert vår korrupsjonsrisikoanalyse, hvor det er identifisert risikoer knyttet til blant annet gaver og representasjon, interessekonflikter, anskaffelsesprosesser i offentlig sektor, og oppfølging av tredjeparter. På bakgrunn av analysen har vi etablert og videreført mandatorisk antikorrupsjonsopplæring for alle ansatte, med tilleggsmoduler for roller med høyere risiko (salg, innkjøp, ledelse og partneransvarlige).

Varslingskanal

Ansatte, leverandører og andre interessenter kan varsle om kritikkverdige forhold gjennom selskapets eksterne varslingskanal, [Whistleblowing](#). Kanalen sikrer mulighet for anonym varslings og uavhengig saksbehandling. Det har ikke vært behandlet saker gjennom varslingskanalen som omhandler brudd på grunnleggende menneskerettigheter eller anstendige arbeidsforhold i rapporteringsperioden.

Håndtering av informasjonskrav

Enhver har, etter åpenhetsloven § 6, rett til å be om informasjon om hvordan House of Control håndterer faktiske og potensielle negative konsekvenser for grunnleggende menneskerettigheter og anstendige arbeidsforhold. Henvendelser kan rettes skriftlig til post@houseofcontrol.no og besvares innen rimelig tid og senest tre uker etter mottak, jf. § 7. Bærekraftsansvarlig i House of Control er ansvarlig for å koordinere og besvare informasjonskravene.

Konklusjon og veien videre

House of Control har i rapporteringsperioden ikke avdekket faktiske, negative konsekvenser for grunnleggende menneskerettigheter eller anstendige arbeidsforhold i egen virksomhet eller hos våre nærmeste leverandører. Vårt arbeid har imidlertid bekreftet at det finnes flere potensielle risikoer lenger bak i våre globale leverandørkjeder, særlig knyttet til produksjon av elektronisk maskinvare og drift av datasentre.

Sentrale resultater av aktsomhetsarbeidet i denne perioden:

- Vi har endret leveransemodell for renhold og kantine ved å ansette personell direkte i House of Control, noe som har redusert risikoen vesentlig på et område der bransjen tradisjonelt har høy risiko for uverdige arbeidsforhold.
- Vi har oppdatert vår interne veiledning for aktsomhetsvurderinger av leverandører, med tydeligere ansvars plassering og en strukturert årlig revisjonssyklus.
- Vi har gjennomført en oppdatert korrupsjonsrisikoanalyse for hele virksomheten, med definerte tiltak og risikoansvarlige.
- Vi har gjennomgått og bekreftet at vår globale skyleverandør har tilfredsstillende systemer for å håndtere de indirekte risikoene i sin verdikjede.

Vi erkjenner at aktsomhetsarbeid er en kontinuerlig prosess. I året som kommer vil vi prioritere følgende:

- Videreutvikle systematikken i den årlige revisjonen av våre mest vesentlige leverandører, herunder klarere kriterier for når dialog eller tiltak skal initieres.
- Tettere integrasjon mellom aktsomhetsvurdering og innkjøpsprosessene, slik at risiko vurderes før kontrakt inngås.
- Følge utviklingen av EU-regelverk, særlig Corporate Sustainability Due Diligence Directive (CSDDD), og sikre at vårt rammeverk er rustet for fremtidige krav.
- Videreføre og styrke opplæringen av ansatte i etikk, antikorrupsjon og ansvarlig forretningsdrift.

Vi vil fortsette det systematiske arbeidet med å forbedre våre aktsomhetsvurderinger og følge opp våre leverandører i året som kommer.

Høvik, 30. juni 2026

For House of Control AS

Daglig leder

House of Control AS

Styreleder

House of Control AS

Styremedlem

House of Control AS

Styremedlem

House of Control AS


Redegjørelsen er signert elektronisk i tråd med regnskapsloven § 3-5. Signaturer fremgår av vedlagt signaturark.

Redegjorelse_apenhetsloven_2026 .docx.pdf

Name
Grønlund, Julie Katrine Groth Date
2026-05-11

Document ID
9e1945d2-5244-4f16-945a-894d9032aa74

Identification

 Grønlund, Julie Katrine Groth

Name
Karlsson, Christina Date
2026-05-12

Document ID
9e1945d2-5244-4f16-945a-894d9032aa74


Identification

 Karlsson, Christina

Name
Sommerseth, Martin Hagen Date
2026-05-12

Document ID
9e1945d2-5244-4f16-945a-894d9032aa74

Identification

 Sommerseth, Martin Hagen

Name
Friis, Kjartan Nielsen Date
2026-05-12

Document ID
9e1945d2-5244-4f16-945a-894d9032aa74

Identification

 Friis, Kjartan Nielsen



This document contains electronic signatures using EU-compliant PAdES - PDF
Advanced Electronic Signatures (Regulation (EU) No 910/2014 (eIDAS))